

Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C.

RECEIVED

FEB 10 1994

FEDERAL COMMUNICATIONS COMMISSION  
OFFICE OF THE SECRETARY

In the Matter of )

Policies and Rules Concerning )  
Toll Fraud )

CC Docket No. 93-292

REPLY COMMENTS OF GTE

GTE Service Corporation and its affiliated  
domestic telephone, equipment and service  
companies

David J. Gudino  
1850 M Street, NW  
Suite 1200  
Washington, DC 20036  
(202) 463-5212

February 10, 1994

Their Attorney

No. of Copies rec'd  
List A B C D E

4

## TABLE OF CONTENTS

	<u>PAGE</u>
SUMMARY .....	iv
DISCUSSION .....	1
I.     LIABILITY FOR PBX FRAUD SHOULD REMAIN WITH THE PBX OWNER.....	1
II.    THE FLORIDA PUBLIC SERVICE COMMISSION PLAN IS NOT A VIABLE SOLUTION TO PRIVATE PAYPHONE TOLL FRAUD .....	7
A. The mere purchase of LEC blocking and screening services alone should not be the sole measure of what constitutes "reasonable" fraud prevention measures by private payphone providers .....	7
B. The network is not the best place to prevent private payphone toll fraud.....	9
C. The financial viability of an entity should have no bearing on liability for payphone toll fraud.....	10
D. The FPSC Plan will not prevent private payphone toll fraud.....	11
E. LECs already have incentives to prevent payphone toll fraud .....	12
III.   THE TOOL MOST NEEDED BY CELLULAR SERVICE PROVIDERS IN THEIR BATTLE AGAINST TOLL FRAUD IS BROADER AND TOUGHER LEGISLATION.....	16
IV.    LINE INFORMATION DATA BASE FRAUD .....	17
A. LIDB owners are actively involved in detecting and preventing calling card toll fraud.....	17
B. The effectiveness of a LIDB in limiting calling card toll fraud is dependent on inputs from, and cooperation by, everyone involved in using or handling calling card calls .....	18
C. LIDB owners should not be required to compensate IXCs for called and calling number information .....	20

D. LIDB owners should not be liable for calling card toll fraud that is beyond their control.....	21
E. Commission action should be limited to requiring that IXCs and OSPs query a LIDB with every calling card call, and provide called and calling number information .....	23
V. COMMISSION INVOLVEMENT CAN PROVIDE VALUABLE ASSISTANCE TO ONGOING INDUSTRY EFFORTS.....	25
A. The Commission should assume the lead in promoting new federal anti-fraud legislation .....	25
B. The Commission should endorse the creation of an be an active participant in an industry panel designed to function as a central source for toll fraud assistance, information and education .....	26

## SUMMARY

Liability for PBX toll fraud should remain with the PBX owner. The PBX owner exercises total control over its PBX. The PBX owner selects the equipment to be installed, enables the fraud prevention features desired, and has the best knowledge of allowable or normal calling patterns when monitoring for suspected fraudulent usage. There are a number of PBX fraud prevention techniques available that should reasonably be deployed. In the context of toll fraud, ignorance cannot be allowed to constitute "bliss". Claims of ignorance regarding PBX toll fraud or ways to prevent it ring hollow and should not justify any shifting of liability for losses. PBX owners should not be allowed to reap the financial benefits of owning a PBX while shifting its potential financial detriments to others.

With respect to private payphones, LEC blocking and screening services are not the only toll fraud prevention methods available to providers. Establishing the subscription to such services as the only measure of "reasonableness" in preventing toll fraud will only undermine the overall of fraud prevention effort. The FPSC Plan ignores this fact -- the Commission should not.

Shifting the responsibility for toll fraud losses from private payphone providers to network providers simply because the network is being used to complete calls ignores the fact that it is the private payphone provider who is furnishing the initial access to the network. Because it controls the mode of access and is in the best position to detect fraudulent use, it must be held responsible for the manner in which it exercises that control. If a private payphone provider lacks the resources necessary to take all reasonable toll fraud precautions or to survive the impact of a loss or losses from toll fraud, it

Deployment of the FPSC Plan has not resulted in any significant decline of toll fraud in Florida. It has only squelched the complaints of private payphone providers by shifting liability for losses away from them to the LECs and IXCs. Implementation of the FPSC Plan on a national level would result in a substantial amount of resources being devoted to resolving disputes over liability as the amounts at stake would increase significantly. These resources would be better used in battling toll fraud itself rather than its aftermath.

Toll fraud is expensive for all parties affected by it. LECs incur costs when private payphone providers are subjected to toll fraud even when it is not required to absorb the losses. Investigating and resolving toll fraud problems is costly and serves as an incentive to the LECs to prevent toll fraud whenever possible. As a result, GTE has been and will continue to work with its customers, including private payphone providers, to prevent toll fraud.

The tool most needed by cellular service providers in their battle against cellular fraud is broader and tougher federal legislation. Heavy-handed outside involvement would only dissipate the momentum the cellular industry has built up in its efforts against fraud.

There are a number of existing financial incentives that motivate LIDB owners to actively engage in the fighting against calling card toll fraud. However, a LIDB cannot prevent calling card toll fraud. It can only aid in detecting fraudulent activity and limiting resulting losses. The effectiveness of LIDB detection capabilities is highly dependent on it actually being used and on complete information being provided to it, such as called and calling number data.

LIDB owners should not be assigned any liability for calling card fraud that is beyond their control. However, should the Commission decide to allocate liability in this manner, the resulting increase in costs must be passed on to LIDB

LIDB owners should not be assigned any liability for calling card fraud that is beyond their control. However, should the Commission decide to allocate liability in this manner, the resulting increase in costs must be passed on to LIDB customers in the form of higher LIDB query rates. In no event should the LIDB owner's liability for fraudulent calls exceed its total revenues from them.

LIDB owners should not be required to compensate IXCs for providing called and calling number information with a LIDB query. The costs are minimal and the benefits accrue directly to the party providing the information. Inclusion of costs for called and calling number information in LIDB rates would result in additional administrative expenses with no net revenue difference to anyone.

IXCs and OSPs should be required to query a LIDB on every call, and provide called and calling number information. The Commission should not mandate standardized LIDB operational procedures as they could be too costly and inflexible for LIDB owners.

Finally, the Commission must lead the industry in its effort to lobby Congress for badly needed new anti-fraud legislation. The comments make it clear that until new laws are enacted, toll fraud prosecutions will continue to meet with only sporadic success. In addition, the Commission should endorse the creation of and actively participate in an industry panel designed to function as a central source for toll fraud assistance, information and education

Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554

RECEIVED

FEB 10 1994

FEDERAL COMMUNICATIONS COMMISSION  
OFFICE OF SECRETARY

In the Matter of )

Policies and Rules Concerning )  
Toll Fraud )

CC Docket No. 93-292

### REPLY COMMENTS OF GTE

GTE Service Corporation ("GTE"), on behalf of its affiliated domestic telephone, equipment, and service companies, offers its Reply Comments to the Comments of other parties filed in response to the Commission's Notice of Proposed Rulemaking ("NPRM") in the above-captioned matter, released December 2, 1993, FCC No. 93-496.<sup>1</sup>

### DISCUSSION

#### **I. LIABILITY FOR PBX FRAUD SHOULD REMAIN WITH THE PBX OWNER.**

Most (if not all) companies purchase a PBX in the belief that it will save them money on their telecommunications expenses. In making this business decision, factors such as the price of the equipment, the cost of installing and maintaining it, and the cost of educating employees on the proper and allowable uses of the equipment must be considered. Whether PBX users like it or not, the potential for PBX fraud and the associated prevention and detection costs also must be considered.<sup>2</sup> The Commission must not allow claims of ignorance about

---

<sup>1</sup> The names of commenters have been abbreviated herein. Their full names appear in Attachment A.

<sup>2</sup> Ignoring this factor is akin to considering every factor in purchasing a new car except insurance.

available PBX toll fraud prevention and detection measures to justify the release of PBX owners from full responsibility for the equipment they operate. PBX owners should not be allowed to reap the financial benefits of PBX use while passing the financial detriments on to other users of the network.

The key word associated with PBX toll fraud liability is control.<sup>3</sup> The comments<sup>4</sup> clearly establish that PBX owners alone control their equipment and thus are in the best position to prevent toll fraud.<sup>5</sup> As AT&T (at 11) explains:

Only the customer knows the complete package of CPE products, features and associated software it has purchased, and only the customer has direct access to such equipment. Moreover, the customer is the only party who can monitor all traffic passing through its PBX and authoritatively determine whether any specific call or calls are fraudulent. Thus, the customer alone is in a position to identify fraudulent calls and to re-program its equipment and associated software to shut down or modify the features that have permitted such calling to occur.

As GTE explained in its comments (at 4), modern PBXs have virtually all of the sophisticated capabilities found in exchange carrier end office switches. This is confirmed by Northern Telecom (at 5-6) which lists a number of features its PBXs have to combat toll fraud.<sup>6</sup> Ericsson (at 4) lists a number of measures,

---

<sup>3</sup> In this regard, the Commission (NPRM at ¶13) itself recognizes that control has "shifted from carriers to individual consumers."

<sup>4</sup> See AT&T at 10-11; MCI at 5; WilTel at 3; CompTel at 2; TFS at 4; TRA at 5-6; US WEST at 7; Pacific at 11; SWBT at 3; Rochester at 5; NYNEX at 17; Bell Atlantic at 3 n.3; Ericsson at 3; Northern Telecom at 2; Stephen Satchell at 7.

<sup>5</sup> Obviously some parties, in particular PBX owners, do not agree with this statement although the Utilities Telecommunications Council (at 6) does admit that the PBX owner "should be obligated to employ reasonable measures" and "be under a duty of reasonable care to prevent unauthorized access...by enacting and following internal security/control measures."

<sup>6</sup> These include: requiring user passwords and user names to permit logging onto a system; maintenance terminals that can track activity; control of authorization codes that can be used from a given telephone set; suppression of calling card numbers on Call Detail Recording

in addition to customer premises equipment ("CPE") based security features, that PBX owners can take: exercising adequate supervision over PBX equipment, employees and agents; taking advantage of carrier services to protect against toll fraud; and taking advantage of educational opportunities offered by equipment manufacturers. TRA (at 6) similarly lists many specific fraud prevention techniques available on PBXs and concludes:

An end user's failure to take reasonable steps to prevent toll fraud should be deemed an assumption by it of the risk of such fraud. Any other approach would eliminate the end user's incentive to take affirmative actions to prevent or minimize toll fraud.

GTE agrees with this assessment and that of Ericsson (at 4) that "responsible supervision by the owner and operator over its CPE will eliminate, to the greatest extent possible, the bulk of PBX toll fraud."

Most of the reasons cited by those advocating the arbitrary shift of liability from PBX owners to others focus on cost, lack of properly trained personnel to manage the PBX, lack of education and the basic inability to prevent all fraud.

Pinellas County (at 3-4) states:

While warnings to customers are meritorious...they constitute only a partial remedy for telephone-system-literate customers, and at best an illusory remedy for the average customer, constituting the majority of users in this country. The less sophisticated customer is at the mercy of its own innocence and ignorance....

Pinellas County (3-4) also states: "While we are in agreement that the customer should take security steps commensurate with its understanding of the telephone system and the risks of telephone fraud, certain security measures are beyond

---

printouts; limits on the number of invalid attempts to access mailboxes with locking capabilities after a certain threshold is met; and activating Direct Inward System Access ("DISA") only after a specific request by the customer. These and other features are designed to force the PBX owner to make conscious decisions about security features activated on the PBX.

the economic means of some customers." This theme is echoed by NATA (at 8):<sup>7</sup>

It is unrealistic to expect each of hundreds of thousands of business users, who generally have no particular telecommunications expertise, to take the time to educate themselves about fraud, to try to figure out what they need to add to their CPE or network services in order to prevent as much fraud as possible, and to spend the money to bring each of their individual locations up to state-of-the-art fraud protection.

One of the more important points raised by GTE in its comments is the need for greater education and information sharing regarding toll fraud. It is *not* unrealistic to expect business users to take the time to avail themselves of information regarding prevention and detection techniques. On the other hand, every user should not be expected to always be at the cutting edge of toll fraud prevention and detection technology. The battle against toll fraud must be tempered by reasonableness. And reasonableness does not require that a PBX owner spend inordinate sums of money to shield its PBX, for at some point, the marginal benefits will outweigh the additional costs. Nor does it countenance, however, the maintenance of ignorance through the artificial insulation of owners from liability. In the battle against toll fraud, ignorance cannot be allowed to constitute "bliss."

In making the economic decision purchase a PBX the business owner must consider factors such as funding for fraud prevention and detection technology, funding for educating personnel in the maintenance and supervision of the PBX, and the risks associated with potential toll fraud. It is the sole responsibility of the business owner to resolve these issues before purchasing a PBX. As US WEST (at 39) aptly explains, PBX purchasers

---

<sup>7</sup> NATA is speaking as the representative of equipment vendors.

should be expected to either pay for fraud control up front (*i.e.*, necessitating, perhaps a larger initial investment than might be desirable) or should be expected to pay for the fraud if, and when, it occurs after the fact. The protection and responsibility for fraud losses are properly determined to be one of the myriad costs of doing business for a business.

An arbitrary shift of PBX toll fraud losses from the PBX owner to the exchange carrier would be a gross injustice and would not serve to correct underlying conditions allowing the toll fraud to take place. It also would result in the imposition of toll fraud losses on customers that have acted responsibly, for as WilTel (at 3) points out, "[c]ustomers who take preventative steps would subsidize those who failed to do so." TFS (at 6) notes that "it is undesirable to shift PBX theft expenses to ratepayers in general, who are not in a position to mitigate PBX fraud risks."

With respect to "hacking," Pinellas County is exactly right when it says that "toll fraud hackers have become ... persistent and creative..." but completely wrong when it advocates the inability of end-users to prevent hacking as a justification for reallocating the losses hacking causes to others. Homeowners cannot completely prevent burglaries or arson. Businesses cannot completely prevent pilferage or embezzlement. Car drivers cannot completely prevent traffic accidents. The best any of them can do is evaluate their risk and protect themselves as best as possible. Shifting their potential losses to others simply is not an option. PBX owners victimized by "hacking" are no different and deserve no special treatment. For obvious reasons, imposing PBX toll fraud losses on parties other than the PBX owners makes no practical or economic sense to anyone except PBX owners.

With regard to Centrex toll fraud,<sup>8</sup> GTE offers an array of prevention and detection features. GTE's account managers work with their customers in

---

<sup>8</sup> See ACUTA at 2; NATA at 15.

determining the features best suited to each customer's particular circumstances. GTE's Centrex offerings include many call blocking features that a customer *may* elect to use; e.g., 1+, 0+, 10XXX+, and 900/976. The operative word is "may," as the customer makes the decision on which features will be enabled on its particular system. In order to prevent remote access fraud, GTE's Centrex offering does not include the DISA feature. However, GTE will provide DISA on its Centrex systems at the request of the customer when technically possible.<sup>9</sup> When DISA is provided, GTE alerts the customer to the fraud potential associated with this type of access. In the end, the customer must balance its need for DISA against the risk it presents for toll fraud. Because fraud perpetrated via remote Centrex access is not the result of an exchange carrier's equipment malfunctioning, exchange carriers should not be saddled with the resulting losses.

*In summary:* The PBX owner exercises total control over its PBX. The PBX owner selects the equipment to be installed, enables the fraud prevention features desired, and has the best knowledge of allowable or normal calling patterns when monitoring for suspected fraudulent usage. There are a number of PBX fraud prevention techniques available that should reasonably be deployed. In the context of preventing toll fraud, ignorance cannot be allowed to constitute "bliss." Claims of ignorance regarding PBX toll fraud or ways to prevent it ring hollow and should not justify any shifting of liability for losses. PBX owners should not be allowed to reap the financial benefits of owning a PBX while shifting its potential financial detriments to others.

---

<sup>9</sup> This feature is not offered when the Centrex system resides on a switch that does not have DISA capabilities.

## **II. THE FLORIDA PUBLIC SERVICE COMMISSION PLAN IS NOT A VIABLE SOLUTION TO PRIVATE PAYPHONE TOLL FRAUD.**

The comments of Private Payphone Providers ("PPPs") reflect overwhelming support for the Florida Public Service Commission's Plan ("FPSC Plan"). No other reaction could be expected. The FPSC Plan completely absolves PPPs from payphone toll fraud liability if they take no action other than to subscribe to local exchange carrier ("LEC") blocking and screening services. As discussed below, the record clearly shows that the FPSC Plan is deficient and should not be adopted by the Commission.

### **A. The mere purchase of LEC blocking and screening services alone should not be the sole measure of what constitutes "reasonable" fraud prevention measures by private payphone providers.**

The NJPA (at 1) asserts that "[i]f a payphone operator has availed itself of the call screening services provided by the LEC, it should not be liable for fraudulent calls." The MPA (at 2) takes a milder approach by asking the Commission to establish "reasonable steps" while making it clear that these steps "should not be exhaustive" as a lengthy list "would put an unreasonable and unfair burden on individual competitive providers." IPANY (at 9) states that the "initial burden in preventing toll fraud should rest with Independent Payphone Providers." However, IPANY's "initial burden" would be met simply by purchasing LEC blocking and screening services for, in IPANY's view, "the IPP has no other reasonable opportunity to prevent fraud." APCC (at 24-25) feels that "[r]egardless of who ultimately is charged with the costs of fraudulent use of the network, the Commission must rule that when IPPs have purchased services that are designed to prevent fraudulent calls, they have taken reasonable steps to protect themselves and are not liable for fraudulent telephone charges."

The argument that subscribing to LEC blocking and screening services is the only "reasonable step" that PPPs can take to prevent toll fraud is not supported by the facts. LEC blocking and screening services are only one form of toll fraud prevention and/or detection that can be used by PPPs. There are many other measures that PPPs can and should take. This view is supported by MCI which states (at 10):

The Commission already has found that there are steps PPOs can -- and should -- take, (in addition to purchasing OLS and BNS service) to protect themselves against fraud. For example, the Commission determined that aggregators, including payphone providers, should be able to prevent fraudulent domestic direct-dialed calls through a reprogramming of payphones or through the addition of adjunct devices.... In addition, "cuckoo tones" could be installed in premises equipment by PPOs....

NYNEX (at 20) lists additional measures such as:

exercising reasonable care in the selection of payphone locations, adequately testing the efficacy of payphone fraud control features, adequately monitoring use of the payphones, protecting the physical integrity of the payphones and the inside wire which serves them, and removing or relocating those payphones which are experiencing a high incidence of fraud or vandalism. In addition, payphone providers can program their phones ... to block incoming calls.

PPPs must be held responsible for using all reasonable CPE toll fraud prevention measures, not just the basic LEC blocking and screening services.

*In summary.* LEC blocking and screening services are not the only toll fraud prevention methods available to private payphone providers. Establishing the subscription to such services as the only measure of "reasonableness" in preventing toll fraud will only undermine the overall fraud prevention effort. The FPSC Plan ignores this fact -- the Commission should not.

**B. The network is not the best place to prevent private payphone toll fraud.**

Several payphone associations claim that network solutions are the best approach to preventing payphone toll fraud.<sup>10</sup> For example, APCC (at 11) asserts that "the ultimate responsibility for preventing toll fraud should rest on the carriers, not IPP providers." APCC (*id.*) bases this conclusion on its belief that "network safeguards provide a far greater level of prevention with far greater efficiency" and that "toll fraud can only be eliminated if the responsibility is borne by those who have the most control over access to the network." GTE disagrees with these claims.

The fact that the network is the ultimate target of fraud has no bearing on liability. In the context of private payphones, it is the PPPs who furnish the equipment that provides the access to the network, not the LECs or interexchange carriers ("IXCs"). In furnishing this access, the PPPs must assume the responsibility for making the instrument of access as secure as possible from perpetrators of fraud. Once a call reaches the network, it has already passed the point of being blocked and/or screened. If these mechanisms have not stopped the call's progress,<sup>11</sup> the network provider has no means of identifying the call as a fraudulent one. Unusual calling patterns from a particular payphone (*e.g.*, calls to international points or calls of longer than normal duration) or illegal tampering with the phone to gain access must be controlled by the PPPs. The LEC or IXC simply has no way of knowing what is unusual for a particular payphone or if access to the phone has been illegally obtained.

---

<sup>10</sup> See APCC at 10-11; MPA at 1; NJPA at 1; IPANY at 9.

<sup>11</sup> This might occur, for example, if LEC-based services are being used and the IXC, AOS or other service provider incorrectly uses the billing and screening information provided by the LEC service.

*In summary.* Shifting the responsibility for toll fraud losses from private payphone providers to network providers simply because the network is being used to complete calls ignores the fact that it is the private payphone provider who is furnishing the initial access to the network. Because private payphone providers control the mode of access and are in the best position to detect fraudulent use, they must be held responsible for the manner in which they exercise that control.

**C. The financial viability of an entity should have no bearing on liability for payphone toll fraud.**

Some PPPs claim they cannot afford to either employ all necessary fraud prevention measures or assume the liability for toll fraud losses generated through their facilities.<sup>12</sup> APCC (at 2) laments the fact that many PPPs are small businesses that face a serious threat to their continued ability to stay in business when confronted with toll fraud liability.

Whether or not APCC is correct, financial viability is not and should never become a reason for shifting responsibility for toll fraud losses or requiring a more solvent firm to absorb another's losses. The decision to enter the private payphone business must include an analysis of *all* of the associated costs and risks. This analysis should include such things as the cost of purchasing CPE with the necessary fraud prevention and detection features, avoiding locations that might offer high revenue levels but that are unusually susceptible to fraudulent activity, and the potential losses from toll fraud and vandalism. In other words, potential losses from toll fraud must be factored in as just another cost of doing business. Any Commission action that would obviate the need for such an analysis will only undermine the battle against toll fraud in this sector and result in an uneconomic market of payphone providers.

---

<sup>12</sup> See APCC at 2; MPA at 2.

*In summary:* If a private payphone provider lacks the resources necessary to take all reasonable toll fraud precautions or to survive the impact of a loss or losses from toll fraud, it should not be in the business. Lack of financial wherewithal is no reason to shift the burden of payphone toll fraud to the LECs and/or IXC.

**D. The FPSC Plan will not prevent private payphone toll fraud, but it will create an environment rife with disputes over responsibility.**

The most compelling indictment of the FPSC Plan is made by the FPTA (at 3) with its simple statement that "[a]doption of the rule will not solve toll fraud." This is in accord with GTE's contention (at 11-12) that the FPSC Plan does not attack the causes of toll fraud -- it only addresses the after-effects. The FPSC Plan simply reassigns liability for toll fraud from PPPs to LECs and/or IXCs, rather than encouraging involvement by all parties in its prevention. The FPTA (at 7) states that "no litigation or other proceedings have been initiated at the FPSC or in any Florida court and no IXC or LEC has sought to collect from a competitive pay telephone provider charges resulting from such fraudulent calls." This observation is merely a testament to the FPSC Plan's effectiveness in reducing the number of complaints filed by PPPs, not evidence that toll fraud has been reduced. In reality, the losses that once generated the litigation and "other proceedings" by the PPPs are now being absorbed by the LECs and IXCs.

Determinations as to why toll fraud is occurring is not happening in Florida. These determinations are not easily made and, in large part, are more costly to make than the dollar value of the resulting losses, especially since only intrastate toll fraud is at issue. This situation will definitely change if interstate and international toll fraud, which are the bulk of toll fraud, become part of the liability assessment. Because toll fraud cannot be completely prevented, when

interstate and international toll fraud losses are included in any liability assessment, an environment rife with disputes will emerge. As Sprint (at 9) predicts:

Any rule which attempts to identify which party is liable for toll fraud costs under different scenarios, and any formula which attempts to apportion liability, are likely to be unworkable. Because the list of toll fraud scenarios could be enormous, any attempt to catalogue the specific conditions under which various parties are liable would be incomplete, will inevitably lead to disputes, and will embroil the Commission in a series of proceedings to determine the extent of each party's culpability.

Teleport (at 4) notes that "there will be clear financial incentives on the part of payphone providers to classify fraudulent calls as the product of deficient screening or validation, and disputes about responsibility can be expected." Resolving these disputes will become an onerous task, further increasing the overall costs associated with toll fraud.

*In summary:* Deployment of the FPSC Plan has not resulted in any significant decline of toll fraud in Florida. It has only squelched the complaints of private payphone providers by shifting liability for losses away from them to the LECs and IXC's. Implementation of the FPSC Plan on a national level would result in a substantial amount of resources being devoted to resolving disputes over liability as the amounts at stake would increase significantly. These resources would be better used in battling toll fraud itself rather than its aftermath.

**E. LECs already have incentives to prevent payphone toll fraud.**

Contrary to APCC's statement (at 8) that "neither LECs nor IXC's have adequate incentives to prevent fraud," LECs have been working for years to prevent toll fraud. Their efforts have been driven by the substantial amounts of

time and money they must expend in investigating fraudulent activity and in dealing with unhappy customers, whether end users or PPPs.

APCC's anemic attempt to convince the Commission that LECs have not been active in payphone toll fraud prevention by describing alleged examples of LEC inadequacies is merely a transparent effort to shift the losses for payphone toll fraud to the LECs. APCC (at 22) discusses "clip-on" fraud, claiming that "it has often been difficult for IPP providers to obtain the LECs' cooperation in securing the network interface." Contrary to this statement, to the extent that GTE has any involvement in locating or securing the network interface, it fully cooperates with its customers.

GTE locates network interface devices in accordance with both FCC rules and National Electrical Code standards.<sup>13</sup> The Commission requires the network interface (or demarcation point) to be located within 12 inches of the network protection device for single line installations.<sup>14</sup> For multiline installations, GTE adheres to the Commission's "minimum point of entry."<sup>15</sup> The National Electrical Code requires telecommunications cables to be protected from voltage surges at every location where service is provided. The network protection device must be grounded and located as close as practicable to the nearest grounding electrode system.<sup>16</sup>

---

<sup>13</sup> The terms "network interface device," "network protection device" and "protector" are essentially synonymous.

<sup>14</sup> *Review of Sections 68.104 and 68.213 of the Commission's Rules Concerning Connection of Simple Inside Wiring to the Telephone Network and Petition for Modification of Section 68.213 of the Commission's Rules filed by the Electronic Industries Association*, Report and Order and Further Notice of Proposed Rulemaking, 5 FCC Rcd 4687, 4692 (1990).

<sup>15</sup> *Id.* at 4693.

<sup>16</sup> See National Electrical Code Handbook, Articles 250-81, 800-30(b), 800-40(b), 800-40(d).

For multiline locations, the network interface, or point of demarcation, is typically a large network protection device provided by GTE that is capable of terminating many lines. This device is normally located in an equipment room or closet or, less frequently, in a lockable case attached to the exterior of a building. GTE has no control over access to these locations or to the building wiring on the customer side of the network interface device. PPPs with payphones located in multiline locations must work cooperatively with building owners, not LECs, to secure the network interface from "clip-ons."

For new simple wiring installations,<sup>17</sup> GTE usually goes beyond the Commission's basic requirement and places a lockable network interface device that includes a network interface jack.<sup>18</sup> If the customer chooses to attach a lock to the network interface device, unauthorized access to the network interface jack and inside wire terminations is greatly diminished. GTE normally installs the network interface device in a location that is convenient for installation and repair personnel to reach. However, at the customer's request, GTE will install the network interface device in a customer selected location as long as both FCC and National Electrical Code requirements are met.

Second dial tone is another issue raised by the private payphone providers.<sup>19</sup> IPANY (at 4) blames alleged LEC equipment "failures" for second dial tone on 800 calls. In fact, however, LEC central office switches are not failing in any manner. They simply were not designed to prevent second dial tone on 800 calls. LEC pay stations also allow second dial tone on 800 calls.

---

<sup>17</sup> One or two line installations.

<sup>18</sup> The only exception is when a new one or two line installation is requested at a location that already has a multiline network protection device in place. Thus, if a PPP requests a line at a building where a multiline network protection device already exists, GTE would not install a new one or two line protection device, but would use the existing multiline device.

<sup>19</sup> See APCC at 21, IPANY at 4.

This is a feature associated with 800 service which many 800 service subscribers rely upon for call completion to other numbers.

APCC (at 20-21) is also concerned with another type of second dial tone created by a "who has control of the circuit issue." BellSouth (at 9) explains: "Secondary dial tone reorigination may be produced in CPE coin telephone equipment which is not manufactured according to digital switch specifications." BellSouth (at 9 n.12) describes situations in which LEC central office switches cannot prevent this secondary dial tone reorigination. GTE recognizes that in certain situations and with certain switch types, it is impossible for the LEC to prevent secondary dial tone reorigination.<sup>20</sup> In switches that can prevent this from occurring, GTE puts all properly identified private payphone lines in a special class of service category that prevents secondary dial tone reorigination.

Finally, some private payphone providers have complained that the "no PIC" option is not available.<sup>21</sup> GTE wishes to note for the record that this option *is* available to the PPPs in its service areas

*In summary:* Toll fraud is expensive for all parties affected by it. LECs incur costs when private payphone providers are subjected to toll fraud even when they are not required to absorb the losses. Investigating and resolving toll fraud problems is costly and serves as an incentive to the LECs to prevent toll fraud whenever possible. As a result, GTE has been and will continue to work with its customers, including private payphone providers, to prevent toll fraud.

---

<sup>20</sup> Older switch types are technically incapable of preventing secondary dial tone reorigination. This does not mean that they have failed, only that they have performed as designed.

<sup>21</sup> See MPA at 3, APCC at 1.

### **III. THE TOOL MOST NEEDED BY CELLULAR SERVICE PROVIDERS IN THEIR BATTLE AGAINST TOLL FRAUD IS BROADER AND TOUGHER LEGISLATION**

An overwhelming number of commenters, favor new federal legislation aimed at making the prosecution of toll fraud easier and the penalties more stringent.<sup>22</sup> As reflected in its comments, GTE firmly believes that tougher legislation is the tool most needed in the battle against cellular fraud. New legislation is needed to define more broadly what constitutes criminal behavior so as to make all existing fraudulent activity subject to its reach and to allow for future applications to the ever-changing ways in which fraud occurs.

GTE does not believe that any form of proactive rule-making committee is needed by the cellular industry. As GTE previously described, cellular service providers have met with considerable success in their ongoing effort against cellular fraud. Heavy-handed outside involvement would only dissipate this momentum. As more fully discussed in Section V.B. below, however, GTE does favor the creation of an industry panel with Commission participation to assist in the coordination of information and the education of all providers and users of telecommunications equipment.

*In summary:* The tool most needed by cellular service providers in their battle against cellular fraud is broader and tougher federal legislation. Heavy-handed outside involvement would only dissipate the momentum the cellular industry has built up in its efforts against fraud.

---

<sup>22</sup> See CTIA at 9; SNET at 3; NYNEX at 23; McCaw at 15; Bell Atlantic at 11.

#### **IV. LINE INFORMATION DATA BASE FRAUD.**

##### **A. LIDB owners are already actively involved in detecting and preventing calling card toll fraud.**

GTE and other Line Information Database ("LIDB") owners are already hard at work combating calling card toll fraud. The comments of LIDB owners document their many on-going efforts which include education of both customers and employees aimed at prevention and detection;<sup>23</sup> implementation of expensive and sophisticated detection systems;<sup>24</sup> and cooperation with customers and other carriers.<sup>25</sup> Commission action in this area is not necessary.

While these ongoing efforts were undertaken "voluntarily," the impetus for them is primarily financial. LEC card issuers are solely liable for intraLATA calling card fraud within their service territory.<sup>26</sup> Additionally, since most LIDB owners also issue calling cards, each seeks to prevent cardholders from becoming "former customers" by preventing unhappy toll fraud experiences.<sup>27</sup> Further, each card issuer must act in a responsible manner to ensure that IXCs continue to accept its card. An IXC always has the option of refusing the calling card of a company that it believes to be negligent in its fraud prevention efforts. And if calling cardholders cannot use one card ubiquitously, they will seek more convenient alternatives. Once a LEC calling card has been abandoned, there is no further opportunity for the LEC to obtain the LIDB query revenues generated in connection with that card. If the LEC's card is replaced with an IXC's card, the LEC also loses the opportunity for revenues from a number of other services

---

<sup>23</sup> See US West at 14-15, 27-29; NYNEX at 4; Pacific Bell at 6-7.

<sup>24</sup> See SNET at 5; NYNEX at 24; SWBT at 11; Pacific Bell at 16-17; Bell South at 11-12.

<sup>25</sup> See Bell Atlantic at 6; NYNEX at 3-4, 6; Pacific Bell at 5; Bell South at 11-12.

<sup>26</sup> See US Intelco at 7.

<sup>27</sup> See GTE at 17; US Intelco at 7-8.

since the customer can then directly access the IXC intraLATA network to use the IXC card.<sup>28</sup>

*In summary:* LIDB owners are already actively engaged in fighting calling card toll fraud. There are a number of existing financial incentives that motivate LIDB owners to work towards limiting calling card fraud.

**B. The effectiveness of a LIDB in limiting calling card toll fraud is dependent on inputs from, and cooperation by, everyone involved in using or handling calling card calls.**

The record is clear on the function of a LIDB in connection with calling card toll fraud. A LIDB toll fraud system can only count how many calls have already been made. It cannot prevent fraudulent calls from being placed. Thus, it can only aid in limiting *future* calling card fraud losses once the existence of fraudulent activity has been detected. And this relatively modest goal can only be achieved if the LIDB is used properly by the LIDB owner and if LIDB customers *use* the LIDB and provide necessary information.

A LIDB is nothing more than a database containing calling card numbers, associated Personal Identification Numbers ("PINs"), and indicators that provide account status and reveal the types of calls permitted to be charged to a particular calling card. The LIDB owner must accept responsibility for proper operation of its LIDB, including the security of PIN number assignment processes, the provision of 24-hour monitoring, maintenance of the accuracy of data inputs, and prompt attention to suspected fraudulent activity, whether discovered by the LIDB owner or another party.

Despite its many features, however, a LIDB cannot prevent calling cards from being lost or stolen, or prevent "shoulder surfing" in busy payphone areas.

---

<sup>28</sup> Revenues lost would include operator service charges and billing, and collection charges as well as the difference between intraLATA access charges and LEC intraLATA toll charges.

Nor can it be effective in detecting calling card fraud unless IXC's and OSP's launch a query for *each and every* call.<sup>29</sup> The three largest IXC's acknowledge the importance of a LIDB query for each call.<sup>30</sup> But even if a query accompanies every call, the LIDB fraud detection system can only identify calling patterns that appear suspicious – it cannot conclusively identify actual fraud. Detecting fraudulent activity at the earliest possible moment, however, can serve to dramatically limit the total amount of potential monetary loss.

There appears to be no dispute that the provision of the called and calling number with a LIDB query is necessary to permit the LIDB owner to fully utilize the detection features of the LIDB system.<sup>31</sup> This information enables different call volume thresholds to be established for various types of calls. Calling card issuers also noted the particular importance of called and calling number information in combating international toll fraud by enabling use of a "Domestic-only" calling card.<sup>32</sup>

Information sharing among LIDB owners and LIDB users could serve to limit calling card toll fraud by alerting potential victims as early as possible and by otherwise allowing each party to learn from the others' experiences. In this regard, IXC's must work toward implementing systems that identify long duration calls, since fraudulent calls are likely to originate in the service territory of a LEC other than the LEC issuing the card, thereby preventing the card issuer from detecting the fraud.<sup>33</sup> LIDB owners and users should also cooperate during

---

<sup>29</sup> See Bell Atlantic at 7; US West at 11; Pacific Bell at 17-18.

<sup>30</sup> See AT&T at 33; Sprint at 18; MCI at 13. However, Bell Atlantic (at 8) reveals that practice does not always follow theory.

<sup>31</sup> See Sprint at 18-19; AT&T at 33; PAPUC at 13; Bell South at 12; US Intelco at 5; SNET at 7; Bell Atlantic at 8; NYNEX at 25 and n.25; US West at 11; Pacific Bell at 16-17.

<sup>32</sup> See Bell Atlantic at 8-9; Bell South at 12.

<sup>33</sup> See Bell Atlantic at 8-9; Bell South at 12.